REMARKS

Claims 1-40 are pending. Claims 1-5, 12-16, 23, 24 and 32 have been amended. Claims 6-8 and 17-19 have been canceled. Claims 1-5, 9-16 and 20-40 remain in the application. No new matter has been introduced.

Claims 1-40 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Application Publication No. 2004/0083384, to Hypponen ("Hypponen"). Applicant traverses the rejection.

A claim is anticipated under 35 U.S.C. §102(e) only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. MPEP §2131. The Hypponen publication fails to teach or suggest each and every claim element and fails to anticipate Claims 1-40.

Hypponen discloses a method of managing a virus signature database associated with an anti-virus application, both of which are resident in a memory of a mobile wireless device (Abstract). Individual signature entries are added, deleted, and replaced to maintain the effectiveness of the virus signature database (¶0007). The Hypponen system is applicable to mobile wireless platforms and devices, such as mobile telephones, communicators, and palmtop and laptop computers with wireless interfaces (¶0008). Management messages, which contain instructions to add, delete or replace the virus signatures, are received by the devices over the wireless interface (¶0010). A sequence number is included in each management message, and each device uses the sequence number to determine whether one or more of the preceding management messages has not been received (¶0011).

Hypponen further discloses filtering the management messages at either the origin side of the wireless interface or at the mobile device to pass only messages relevant to the recipient device (¶0017). The filter has knowledge of the properties of the mobile device and the software applications resident on the mobile device (¶0018). Management messages may contain the identity of mobile devices and the applications to which they are relevant, such that the filter may compare the applicability of messages to the properties or resident software of destination mobile devices (¶0018).

Hypponen further discloses implementing his system in the form of a Public Land Mobile Network (PLMN) that is the home network of a subscriber using a wireless device (¶0024). A management center operated by a third party anti-virus software manufacturer or distributor is coupled to the PLMN and comprises a management server and a management console (¶0025). A human operator sits at the management console and, using the console, is able to send SMS messages to and receive data from mobile devices (¶0025). Each of the wireless devices subscribes to the service of the management center (¶0025). New virus signatures are created at the management center as and when new viruses are detected (¶0032) and causes management messages containing an ADD_NEW_SIGNATURE instruction to be sent to the subscribers (¶0032). All management messages pass through an update filter located at the management server of the management center (¶0033). The filter contains a subscriber database recording the details of applications installed on subscriber devices. Using such information, the filter directs management messages only to those devices to which the messages are appropriate (¶0033).

Independent Claims 1, 12, 24, and 32 have been amended to respectively incorporate the limitations of now-canceled Claims 6-8 and 17-19. No new matter has been entered. Support for the claim amendments can be found in the specification and claims as originally filed.

In contrast, amended Claim 1 specifies "A system for providing telephonic content security service in a wireless network environment" having "a plurality of wireless devices interfacing over a network providing wireless telephonic services through a layered service architecture." Amended Claim 1 further specifies "a status daemon periodically communicating operational data from each wireless device to the network operations center, said operational data being in the form of a report on status and health of the wireless device." Amended Claim 1 further specifies "a network operations center supervising the provisioning of the content security services to each wireless device and maintaining a master catalog of the applications and further maintaining a configured wireless devices list reflecting the status of each wireless device based on the operational data." Finally, amended Claim 1 specifies, "a configuration client managing a configuration of each wireless device by consulting the master catalog and the configured wireless devices list and downloading the applications to each wireless device as required to maintain each wireless device in a most-up-to-date configuration.."

In contrast, amended Claim 12 specifies "A method for providing telephonic content security service in a wireless network environment," and further specifies the steps of "interfacing to a plurality of wireless devices over a network providing wireless telephonic services through a layered service architecture," and "periodically communicating operational data from each wireless device to the network operations center using a status daemon, said operational data being in the form of a report on status and health of the wireless device." Amended Claim 12 further recites the steps of "supervising the provisioning of the content security services to each wireless device from a network operations center at which are maintained a master catalog of the applications and configured wireless devices list reflecting the status of each wireless device based on the operational data" and "managing a configuration of each wireless device from a configuration client by consulting the master catalog and the configured wireless devices list and downloading the applications to each wireless device as required to maintain each wireless device in a most-up-to-date configuration."

In contrast, amended Claim 24 specifies "A system for provisioning a plurality of wireless devices in a closed content security service loop framework," including "a network operations center delivering content security services to each wireless device through the content security service components being executed thereon, and automatically periodically receiving a status report from each wireless device by means of a status daemon, each status report providing status information comprising machine-specific data and application-specific information."

In contrast, amended Claim 32 specifies, "A method for provisioning a plurality of wireless devices in a closed content security service loop framework," including the step of "automatically periodically receiving a status report from each wireless device by means of a status daemon, each said status report providing status information comprising machine-specific data and application-specific information."

In contrast to amended independent Claims 1, 12, 24 and 32, Hypponen fails to teach or suggest independently operating a daemon that automatically obtains actual operating data from each wireless device. Hypponen instead relies on a human operator to direct the sending of management messages to subscribers. Hyponnen further relies on the integrity of records maintained at the management center to determine whether a subscriber device is properly configured. Moreover, Hypponen fails to teach or suggest obtaining real time information directly from each subscriber device to determine its actual configuration. Nor does Hypponen teach or suggest comparing status information obtained directly from devices through an independently operating daemon against a master catalog to determine whether updates are in order.

Therefore, the Hypponen reference fails to describe all the claim limitations and does not anticipate amended Claims 1, 12, 24, and 32. Claims 6-8 and 17-19 have been canceled. Claims 2-5 and 9-11 are dependent on Claim 1 and are patentable for the above-stated reasons and as further distinguished by the limitations recited therein. Claims 13-16 and 20-22 are dependent on Claim 12 and are patentable for the above-stated reasons and as further distinguished by the limitations recited therein. Amended Claim 23 is multiply dependent on Claims 12, 13, 14, 15, 16, 20, 21, or 22 and is patentable for the above-stated reasons and as further distinguished by the limitations recited therein. Claims 25-31 are dependent on amended Claim 24 and are patentable for the above-stated reasons and as further distinguished by the limitations recited therein. Claims 33-39 are dependent on amended Claim 32 and are patentable for the above-stated reasons and as further distinguished by the limitations recited therein. Claim 40 is multiply dependent on Claims 32, 33, 34, 35, 36, 37, 38, or 39 and is patentable for the above-stated reasons and as further distinguished by the limitations recited therein. Withdrawal of the rejection under 35 U.S.C. §102(e) is respectfully requested.

The prior art made of record and not relied upon has been reviewed by the applicant and is considered to be no more pertinent than the prior art references already applied.

Examination and further consideration of the application is respectfully requested. Claims 1-5, 9-16 and 20-40 are believed to be in a condition for allowance. Entry of the foregoing amendments is requested and a Notice of Allowance is earnestly solicited. Please contact the undersigned at (206) 381-3900 regarding any questions or concerns associated with the present matter.

Respectfully submitted,

Dated: March 17, 2005

By: ______________________
Patrick J.S. Inouye, Esq.
Reg. No. 40,297

Law Offices of Patrick J.S. Inouye
810 Third Avenue, Suite 258
Seattle, WA 98104

Telephone: (206) 381-3900
Facsimile: (206) 381-3999

OA Response A